Computing square roots mod $p$

We now have very effective ways to determine \textit{whether} the quadratic congruence $x^2 \equiv a \pmod{p}$, $p$ an odd prime, is solvable. What we need to complete this discussion is an effective technique to \textit{compute} a solution if one exists, that is, if $\left(\frac{a}{p}\right) = 1$. Consequently, for the remainder of this discussion we will assume that $a$ is a quadratic residue mod $p$.

Now it turns out that finding a solution to $x^2 \equiv a \pmod{p}$ is easy if $p \equiv 3 \pmod{4}$: we write $p = 4k + 3$, then set $x \equiv a^{k+1} \pmod{p}$. By Euler’s Criterion,

$$x^2 \equiv a^{2k+2} = a^{2k+1} \cdot a \equiv a^{p-1} \cdot a \equiv \left(\frac{a}{p}\right) \cdot a \equiv a \pmod{p}$$

so $x \equiv a^{k+1} \pmod{p}$ is a solution to the original quadratic congruence. That is, $a^{k+1} \equiv a^{\frac{p+1}{4}} \pmod{p}$ is a square root of $a$ mod $p$.

Of course, this method fails if $p \equiv 1 \pmod{4}$. But we can further differentiate values of $p$ if instead we work mod 8: if $p \equiv 1 \pmod{4}$, then either $p \equiv 1 \pmod{8}$ or $p \equiv 5 \pmod{8}$. 
Consider the latter case, $p = 8k + 5$, first. By Euler’s Criterion, we have that $a^\frac{p-1}{2} \equiv 1 \pmod{p}$, so $a^\frac{p-1}{4} \equiv \pm 1 \pmod{p}$. If $a^\frac{p-1}{4} \equiv 1 \pmod{p}$, then setting $x = a^{k+1} \pmod{p}$ yields a solution since

$$x^2 \equiv a^{2k+2} \equiv a^{\frac{p+3}{4}} \equiv a^{\frac{p-1}{4}} \cdot a \equiv a \pmod{p}.$$ 

If instead, $a^\frac{p-1}{4} \equiv -1 \pmod{p}$, then $x \equiv 2^{2k+1} a^{k+1} \pmod{p}$ yields a solution since

$$x^2 \equiv 2^{4k+2} a^{2k+2} \equiv 2^{\frac{p-1}{2}} a^{\frac{p+3}{4}}$$
$$\equiv \left(\frac{2}{p}\right)^{\frac{p-1}{2}} \cdot a^{\frac{p-1}{4}} \cdot a \equiv -1 \cdot -1 \cdot a \equiv a \pmod{p}.$$ 

We’re still left with the case $p \equiv 1 \pmod{8}$. Now we could continue this development by producing more and more complicated formulas for computing the square root of $a \pmod{p}$, depending on the residue class of $p$ modulo higher and higher powers of 2, but thankfully this is unnecessary, as it is possible to set forth an algorithm that does this systematically.
Write $p - 1 = 2^r s$, with $s$ odd. Taking a cue from the methods discussed above, we suggest that

$$y \equiv a^{s+1} (\mod p)$$

might be a good “first try” at a square root for $a$. Observe that

$$y^2 \equiv a^{s+1} = a^s \cdot a (\mod p)$$

It follows that since both $y^2$ and $a$ are quadratic residues mod $p$, so must $a^s$ be. This reduces our problem to the computation of a square root for $b \equiv a^s (\mod p)$, for if $z^2 \equiv b (\mod p)$, then

$$(yz^{-1})^2 \equiv a^{s+1} \cdot a^{-s} \equiv a (\mod p)$$

and so $yz^{-1}$ is a square root of $a$ mod $p$.

On the face of it, it doesn’t look like we have gained much by transferring the problem of computing a square root $y$ of $a$ to that of computing a square root $z$ of $b$. But indeed we have, since

$$b^{2^{r-1}} = (a^s)^{2^{r-1}} = a^{2^{r-1}} \equiv \left(\frac{a}{p}\right) \equiv 1 (\mod p) \Rightarrow \text{ord}_p b \mid 2^{r-1}$$

so that

$$\text{ord}_p z = 2 \cdot \text{ord}_p b \mid 2^r \Rightarrow \text{ord}_p z \text{ is a power of } 2 \leq 2^r$$

which severely limits the possible values for $z$. 
For those who know some group theory, notice also that the set of nonzero residue classes mod $p$ whose order divides a power of 2 is a subgroup of the group of units mod $p$. That is, if $z_1$ and $z_2$ have orders mod $p$ equal to $2^{n_1}$ and $2^{n_2}$, respectively, then the order of $z_1z_2$ is the larger of $2^{n_1}$ and $2^{n_2}$, hence is also a power of 2; further, the inverse of $y_1$ has order $2^{n_1}$ as well (since $(z^{-1})^{2^r} = (z^{2^r})^{-1} = 1$). In fact, this subgroup is called the 2-Sylow subgroup of the group of units mod $p$.

We will denote the set of elements $y$ whose order mod $p$ is a power of 2 as $S$. (This means that $S$ is the 2-Sylow subgroup of the group of units mod $p$.) It may seem that we would have to turn to finding a primitive root mod $p$ to get at the structure of the elements in $S$, but it turns out to be much easier:

**Lemma** If $n$ is any quadratic nonresidue mod $p$, and $m \equiv n^s \pmod{p}$, then $S = \{m, m^2, m^3, ..., m^{2^r}\}$.

**Proof** By EC, $m^{2^{r-1}} = (n^s)^{2^{r-1}} = n^{\frac{p-1}{2}} = -1 \pmod{p}$. But by Fermat’s Little Theorem, $m^{2^r} = (n^s)^{2^r} = n^{p-1} \equiv 1 \pmod{p}$, so we must have that $\text{ord}_p m = 2^r$. Thus the first $2^r$ powers of $m$ are distinct mod $p$ and all lie in $S$. But as there are $\varphi(2^k)$ elements of order $2^k$, and each of these orders
is a factor of $2^r$, the total number of elements whose order divides $2^r$ is

$$\sum_{k=0}^{r} \varphi(2^k) = \sum_{d|2^r} \varphi(d) = 2^r,$$

hence we have accounted for all the elements of $S$. The result follows. //

Returning to our original problem: to solve $x^2 \equiv a \pmod{p}$, we search instead for a square root $z$ of $b \equiv a^s \pmod{p}$, so that with $y \equiv a^{\frac{s}{2}} \pmod{p}$, we can then compute $x \equiv yz^{-1} \pmod{p}$, which will be the desired square root of $a$ (since $y^2 \equiv z^2a \pmod{p}$). As the order of $b$ divides $2^{r-1}$, $z$ will also lie in $S$ and is thus some power of $m = n^s$, where $n$ is some quadratic nonresidue mod $p$. Indeed, $z \equiv m^k \pmod{p}$ implies that $b \equiv z^2 \equiv m^{2k} \pmod{p}$. That is, $b$ must be some even power of $m$. Halving this even power will locate the desired value of $z$.

Now one way to proceed with finding $z$ is to simply search through all even powers of $m$ until $b$ appears. This will take no more than $r$ steps. But in fact, there is a procedure that will accomplish this without having to calculate the corresponding powers of $m$. It is based on the
Lemma If $\text{ord}_p m = 2^r$ and $\text{ord}_p b = 2^u$ with $u < r$, then $\text{ord}_p (m^{2^{r-u}} b) = 2^v$ with $v < u$.

Proof Since $\text{ord}_p m = 2^r$, we have $m^{2^{r-1}} \not\equiv 1 \pmod{p}$ but $(m^{2^{r-1}})^2 \equiv m^{2^r} \equiv 1 \pmod{p}$, whence $m^{2^{r-1}} \equiv -1 \pmod{p}$. Similarly, $b^{2^{u-1}} \equiv -1 \pmod{p}$. Therefore,

\[(m^{2^{r-u}} b)^{2^{u-1}} \equiv m^{2^{r-1}} b^{2^{u-1}} \equiv (-1)(-1) \equiv 1 \pmod{p},\]

which implies that the order of $m^{2^{r-u}} b \pmod{p}$ must divide $2^{u-1}$. //

The importance of this observation is that if $b = 1$, finding $z$ is trivial, for then $z = 1$. If $b \neq 1$, the lemma allows us to adjust the value of $b$ by multiplication by a perfect square (namely, an even power of $m$), which replaces $b$ with a new value $b' = m^{2^{r-u}} b$ having smaller order than $b$. This adjustment makes it no more difficult to find a square root ($z$ gets “adjusted” by a factor of $m^{2^{r-u-1}}$), but as the order of $b'$ is smaller, it means that $b'$ is in some sense “closer” to 1 (whose order is the smallest possible). By repeating this process, we eventually reach a stage where $b$ has been reduced to 1, and the computation is complete.
We illustrate with some examples:

**Example:** \( x^2 = 2 \pmod{41} \)

Factor \( 41 - 1 = 2^3 \cdot 5 \) (so that \( r = 3 \) and \( s = 5 \)), and put \( y \equiv 2^{\frac{5+1}{2}} \equiv 8 \pmod{41} \) and \( b \equiv 2^5 \equiv 32 \pmod{41} \). We know that \( b \) has order dividing \( 2^{3-1} \); since \( b^2 \equiv 32^2 \equiv -1 \pmod{41} \), \( b \) has order equal to \( 2^2 \). Next, take \( n = 3 \) as a quadratic nonresidue, noting by QR that

\[
\begin{pmatrix} 3 \\ 41 \end{pmatrix} = \begin{pmatrix} 41 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ 3 \end{pmatrix} = -1
\]

and set \( m \equiv 3^5 \equiv 38 \pmod{41} \). We know that \( z \) satisfies \( z^2 = b \pmod{41} \), but by the lemma, multiplication of this last congruence by \( m^{2^{r-u}} \equiv 38^{2^{3-2}} \equiv 9 \pmod{41} \) serves to adjust the value of \( b \) to \( b' = 9b \equiv 1 \pmod{41} \) and adjusts \( z \) by the factor \( m^{2^{r-u-1}} \equiv 38^{2^{3-2}} \equiv 38 \pmod{41} \). Also, note that replacing \( z \) with \( z' = 38z \pmod{41} \) means that

\[ x = yz^{-1} = 8 \cdot 38z^{-1} \pmod{41} \]

Repeating this procedure, we have that \( b' = 1 \pmod{41} \), so a square root is \( z' = 1 \), yielding \( x = 8 \cdot 38 \cdot 1 \equiv 17 \pmod{41} \) in one iteration.
We can make this computation more amenable to automation by organizing the steps as follows (here, $\equiv$ means congruence mod $p$):

Given: $p = 41$  
Initialize: $r = 3$  

$a = 2$  
$s = 5$  

$\quad n \equiv 3$  

$(\frac{3}{41}) = -1$  

$m \equiv 38$  

Iterate (until $u_i = 0$, i.e., $b_i = 1$):

<table>
<thead>
<tr>
<th>$i$</th>
<th>$b_i$</th>
<th>ord$_{41} b_i = 2^{u_i}$</th>
<th>$x_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>32 ($b_0 \equiv a^s$)</td>
<td>$2^2$</td>
<td>$8$ ($x_0 = y \equiv a^{\frac{s+1}{2}}$)</td>
</tr>
<tr>
<td>1</td>
<td>$b_{i+1} = m^{2^{r-u_i}} b_i$</td>
<td>$2^0$</td>
<td>$17(x_{i+1} = 2^{r-u_i-1} x_i)$</td>
</tr>
</tbody>
</table>

The desired solution to the original congruence appears in the lower right cell of the table.
Example: \( x^2 \equiv 7 \pmod{113} \)

Given: \( p = 113 \)  
Initialize: \( r = 4 \)  \( (p - 1 = 2^4 \cdot 7) \)  
\( a = 7 \)  
\( s = 7 \)  
\( n = 3 \)  \( \left( \frac{3}{113} \right) = -1 \)  
\( m = 40 \)  \( (m \equiv n^s) \)

Iterate (until \( u_i = 0 \), i.e., \( b_i = 1 \)):

<table>
<thead>
<tr>
<th>( i )</th>
<th>( b_i )</th>
<th>( \text{ord } b_i = 2^{u_i} )</th>
<th>( x_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(-1 ) (( b_0 \equiv a^s ))</td>
<td>( 2^1 )</td>
<td>( 28 ) (( x_0 = y \equiv a^{\frac{s+1}{2}} ))</td>
</tr>
<tr>
<td>1</td>
<td>( 1 ) (( b_{i+1} \equiv m^{2^{2^{r-u_i}}} b_i ))</td>
<td>( 2^0 )</td>
<td>( 32 ) (( x_{i+1} = m^{2^{2^{r-u_i-1}}} x_i ))</td>
</tr>
</tbody>
</table>

Thus \( x \equiv 32 \pmod{113} \).
Example: $x^2 \equiv 103 \pmod{641}$

Given: $p = 641$  Initialize: $r = 7$  \hspace{1cm} (p - 1 = 2^7 \cdot 5) \\
$a = 103$  \hspace{1cm} $s = 5$ \\
$n = 3$  \hspace{1cm} $\left(\frac{3}{641}\right) = -1$ \\
$m = 243$  \hspace{1cm} ($m \equiv n^s$)

Iterate (until $u_i = 0$, i.e., $b_i = 1$):

<table>
<thead>
<tr>
<th>$i$</th>
<th>$b_i$</th>
<th>ord $b_i = 2^{u_i}$</th>
<th>$x_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>625 ($b_0 \equiv a^s$)</td>
<td>$2^4$</td>
<td>$463$ ($x_0 = y \equiv a^{\frac{s+1}{2}}$)</td>
</tr>
<tr>
<td>1</td>
<td>$-1$ ($b_{i+1} \equiv m^{2^{r-u_i}} b_i$)</td>
<td>$2^1$</td>
<td>$365$ ($x_{i+1} \equiv m^{2^{r-u_i-1}} x_i$)</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>$2^0$</td>
<td>$198$</td>
</tr>
</tbody>
</table>

Thus $x \equiv 198 \pmod{641}$.